datomo®
MOBILE
DEVICE MANAGEMENT

DSGVO-Konformität

Version 18.10.2023 – Aktualisiert 26.02.2025

SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN IN DIESEM HANDBUCH EINGEFÜHRTEN PRODUKTEN UND DIENSTLEISTUNGEN KÖNNEN ÄNDERUNGEN UNTERLIEGEN. ALLE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND EMPFEHLUNGEN SIND RELEVANT, JEDOCH LIEGT DIE VERANTWORTUNG FÜR DIE IMPLEMENTIERUNG UND NUTZUNG DER PRODUKTE UND DIENSTLEISTUNGEN BEI DEN ANWENDERN.

Übersicht

1. DSGVO

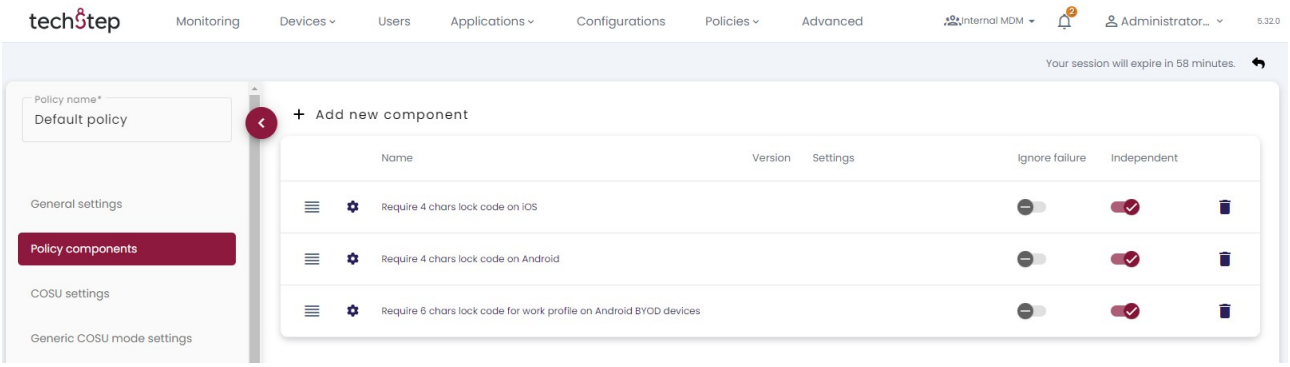
Die Allgemeine Datenschutzverordnung (DSGVO) stellt zusätzliche Anforderungen an den Datenschutz für Organisationen, die personenbezogene Daten verarbeiten und speichern. Um den neuen Vorschriften zu entsprechen, sollten Sie auch die Risiken im Zusammenhang mit der mobilen Datensicherheit analysieren. Organisationen, die ihre mobilen Geräte mit **datomo MDM** verwalten, verfügen über alle erforderlichen Werkzeuge, um die durch das neue Gesetz geforderten Sicherheitsmaßnahmen umzusetzen. Beachten Sie jedoch, dass die DSGVO Leitlinien vorgibt, jedoch keine detaillierten Anweisungen enthält. Letztendlich obliegt es dem Administrator zu entscheiden, welche Sicherheitsmaßnahmen ausreichend sind, um den Anforderungen der Organisation gerecht zu werden.

2. Zugriffskontrolle für mobile Daten

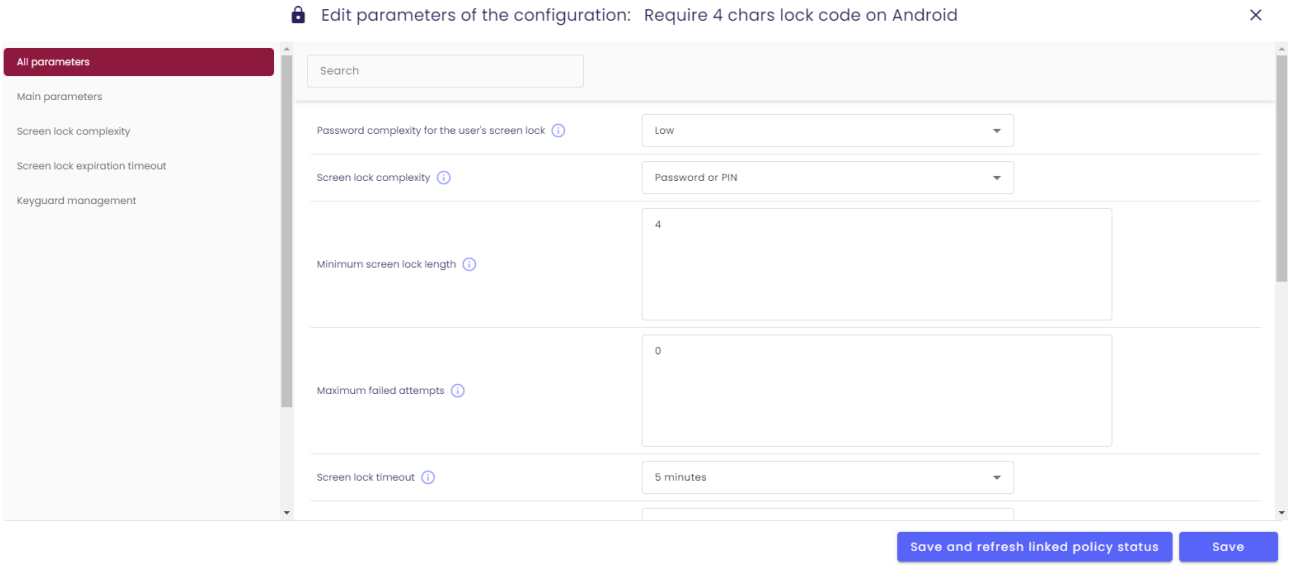
Der Zugriff auf auf einem mobilen Gerät gespeicherte Daten kann auf verschiedene Weise geschützt werden. Die grundlegende Sicherheit kann durch die Festlegung eines Sperrcodes erreicht werden: Das **datomo MDM**-System erzwingt den Sperrcode durch eine Konfiguration, die später der Richtlinie hinzugefügt werden kann. Auf diese Weise kann die Organisation sicherstellen, dass mobile Geräte, die in **datomo MDM** registriert sind, einen Sperrcode benötigen.

Der Geräte-Sperrcode ist eine Standardvorgabe und auch ein Bestandteil der Standardrichtlinie in **datomo MDM**. Der Sperrcode kann mit jeder Richtlinie in der Organisation durchgesetzt werden.

Gehen Sie zu den Richtlinieneinstellungen und fügen Sie die Sperrcode-Konfiguration unter dem Tab „**Richtlinienkomponenten**“ hinzu.



Die Anforderungen an den Sperrcode können durch Bearbeiten der Konfigurationen für eine bestimmte Plattform im Tab „Konfigurationen“ geändert werden, z. B. für die Android-Plattform: „Erfordere einen 4-stelligen Sperrcode auf Android“.

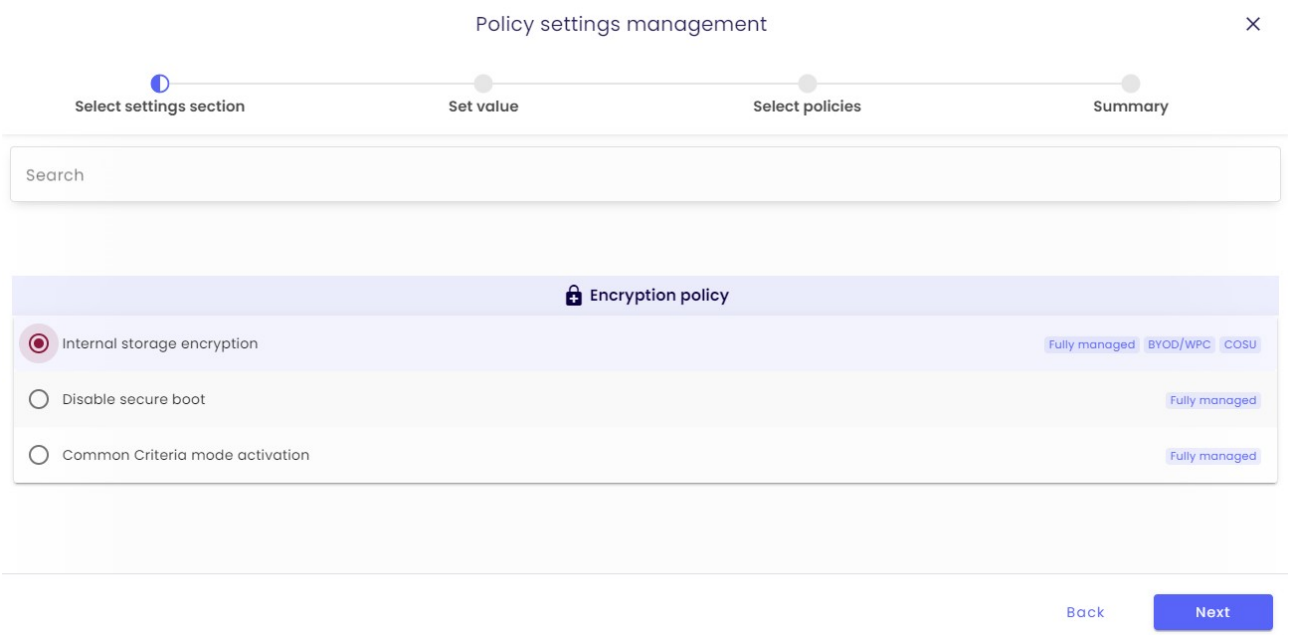


Eine weitere Möglichkeit, die Datensicherheit auf einem mobilen Gerät zu erhöhen, ist die Verschlüsselung des internen Speichers. Geräte, die mit Android 6.0 oder höher oder mit iOS 10 und höher ausgeliefert werden, verfügen über eine eingebaute Verschlüsselung des internen Speichers. Um jedoch die auf einem mobilen Gerät gespeicherten Daten vollständig zu schützen, wird empfohlen, den Sperrcode als zusätzliche Möglichkeit zur Verschlüsselung der Daten durchzusetzen.

Alle Geräte mit Android-Versionen vor 6.0 müssen durch den Prozess der Durchsetzung der internen Speicherverschlüsselung gehen. Während dieses Prozesses muss der Sperrcode eingerichtet werden.

Die Verschlüsselung kann durch Auswählen eines Kontrollkästchens in einer Sicherheitsrichtlinie erzwungen werden:

Richtlinien > Einstellungen ändern > Verschlüsselungsrichtlinie und wählen Sie „Interne Speicherverschlüsselung“ aus.



***Hinweis**: Jede Änderung der Richtlinie muss aktualisiert werden, um angewendet zu werden.*

3. Trennung von Unternehmens- und privaten Daten

3.1. Android-Geräte

Mit **datomo MDM** können Unternehmensdaten von privaten Daten durch Containerisierung getrennt werden. Die Containerlösung ist mit Android Enterprise Work-Profilen (alle Android-Geräte ab Version 7.0) verfügbar.

Zwei Schlüsselelemente zur Verhinderung von Datenlecks bei der Nutzung von Containern sind das Blockieren des Datentransfers (Kopieren - Einfügen) zwischen den Unternehmens- und privaten Umgebungen sowie das Blockieren des Zugriffs auf bestimmte Anwendungen (z. B. Kalender oder Kontakte).

Einstellungen können in der Richtlinie des Unternehmensprofils geändert oder blockiert werden:

Richtlinien > Einstellungen ändern > Einschränkungen des Arbeitsprofils

3.2. Apple-Geräte

Bei iOS-Geräten werden Unternehmensdaten standardmäßig vom Privaten getrennt, wenn das **datomo MDM**-Profil auf dem Gerät installiert ist. Zudem kann der Zugriff auf Unternehmensdaten so eingeschränkt werden, dass nur Unternehmensanwendungen, die durch **datomo MDM** verwaltet werden, auf dem Gerät installiert werden können (nur im Supervised-Modus). Beispielsweise kann ein Anhang, der von einem Unternehmens-E-Mail-Konto heruntergeladen wurde, nur von einer App geöffnet werden, die von der Sicherheitsabteilung genehmigt wurde. Der Zugriff auf Geschäftskontakte kann ebenso auf ähnliche Weise eingeschränkt werden.

Um dies zu erreichen, sollten folgende Parameter geändert werden:

- „Nicht zulassen, dass verwaltete Dokumente über AirDrop geteilt werden“ auf „Nein“
- „Nicht zulassen, dass Daten aus nicht verwalteten Apps geteilt werden“ auf „Nein“
- „Nicht zulassen, dass Daten aus verwalteten Apps geteilt werden“ auf „Nein“

Diese Parameter finden Sie in
Richtlinien > Einstellungen ändern > Anwendungsbeschränkungen.

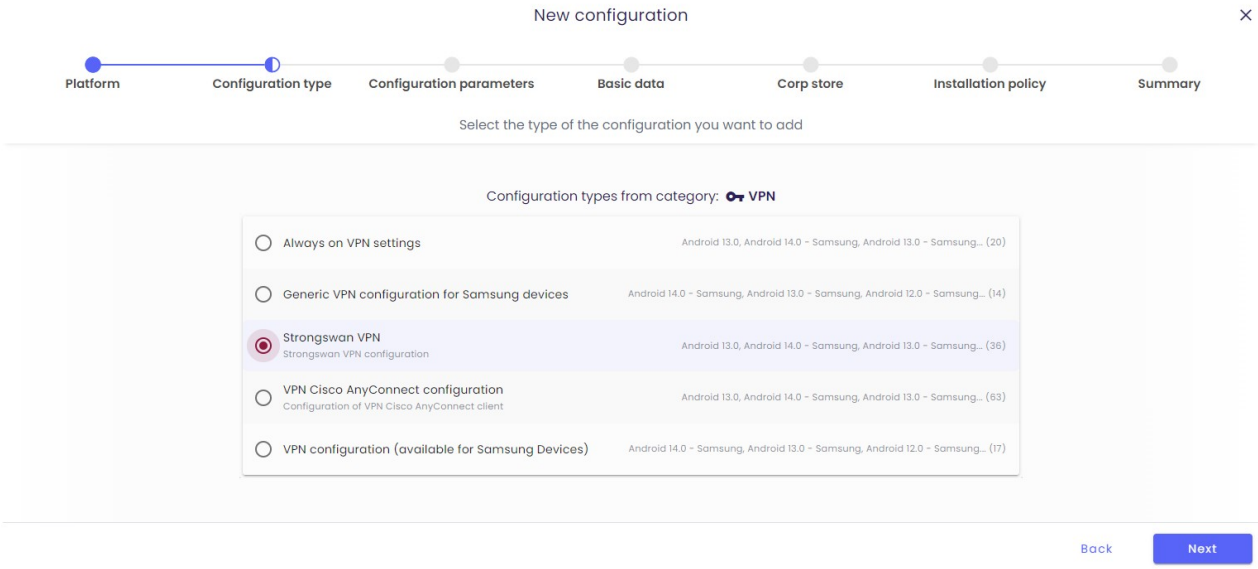
4. Zugriff auf Unternehmensressourcen für Geräte im Außendienst

Daten, die auf Geräten gespeichert sind, die im Außendienst verwendet werden, müssen ebenfalls geschützt werden. Es ist zu beachten, dass mobile Geräte Zugang zum Firmennetzwerk und seinen Ressourcen gewähren. Um sicheren Zugriff auf das Unternehmensnetzwerk zu gewährleisten, wird empfohlen, mit dem **datomo VPN-Netzwerkgateway**, das auf dem IPsec IKEv2-Protokoll basiert, zu integrieren.

datomo MDM hilft Ihnen, zu entscheiden, welche Anwendungen eine VPN-Verbindung nutzen sollen (Per-App VPN). Es kann auch den VPN-Einsatz auf dem gesamten Gerät oder nur auf dem Container (geschäftlicher Teil des Geräts) erzwingen.

4.1. Android-Geräte

Auf Android-Geräten müssen Sie Strongswan VPN über das **datomo EMM** installieren. Die Strongswan-Konfiguration finden Sie unter:
Konfigurationen > Neue hinzufügen > Android > VPN > Strongswan VPN.



In dieser Konfiguration können Sie entscheiden, welche Anwendungen eine VPN-Verbindung benötigen. Wenn die VPN-Verbindung für das gesamte Gerät genutzt werden soll, verwenden Sie die Konfiguration in der allgemeinen Standardrichtlinie. Wenn Sie sie nur auf den Container anwenden möchten, muss sie als Bestandteil einer BYOD/WPC-Richtlinie eingerichtet werden.

4.2. Apple-Geräte

Auf Apple-Geräten verwenden wir den nativen VPN-Client, der in der Apple VPN-Konfiguration eingerichtet werden kann, die Sie unter finden:
Konfigurationen > Neue hinzufügen > Apple > iOS, iPadOS oder macOS > VPN.

„Per-App VPN verwenden“ ermöglicht es Ihnen, Anwendungen und Safari-Webdomains festzulegen, die eine VPN-Verbindung erfordern.

5. Zugriff auf Unternehmensressourcen

5.1. Zugriff auf Unternehmensressourcen im Wi-Fi

Mit der Integration des **datomo MDM**-Systems in die Netzwerk-Infrastruktur des Unternehmens kann das Unternehmen zusätzliche Kontrolle über Geräte erhalten, die versuchen, sich mit dem internen Netzwerk zu verbinden. Nur Geräte, die verwaltet und gesichert sind, dürfen auf das Unternehmensnetzwerk zugreifen. Die Compliance-Verifizierung ist möglich, wenn **datomo MDM** als externer Compliance-Prüfer in **CISCO ISE** oder **Extreme Networks** integriert ist.

5.2. Sicherer Zugriff auf die Unternehmens-E-Mail

Der **datomo Exchange ActiveSync Proxy** gewährt nur verwalteten, gesicherten und **datomo MDM**-konformen Geräten Zugang zu den E-Mail-Servern des Unternehmens. Auf diese Weise kann das Unternehmen sicherstellen, dass kein externes Gerät auf die E-Mails des Unternehmens zugreifen kann. Falls ein unbefugter Zugriff versuchte, wird der **datomo MDM**-Administrator über solch einen Vorfall benachrichtigt.

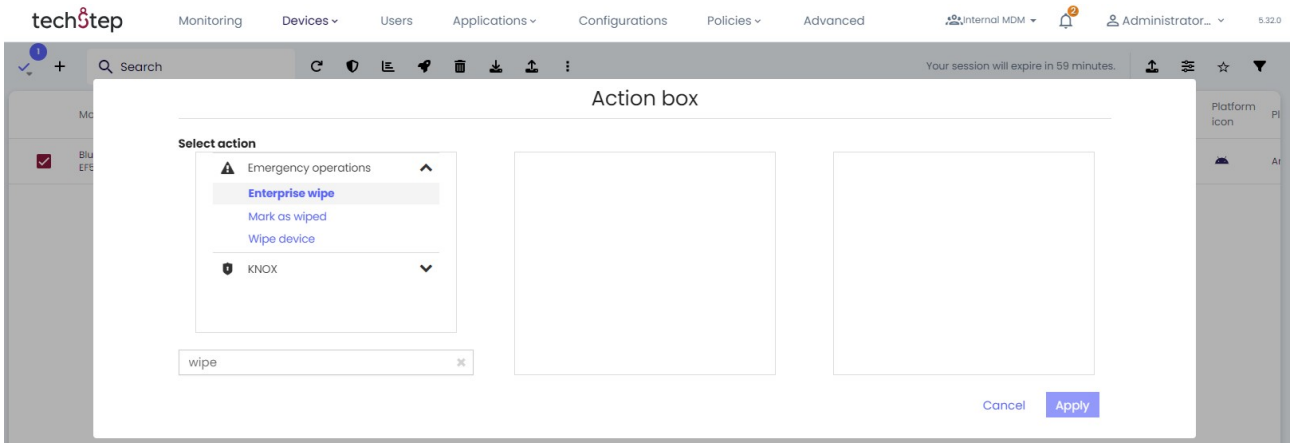
6. Verhinderung von Datenlecks

Im Falle eines Diebstahls oder Verlusts eines Geräts sollte der Mitarbeiter den Vorfall dem IT-Administrator des Unternehmens melden. Geräte, die von **datomo MDM** verwaltet und gesichert werden, stellen keine Gefahr eines Datenlecks dar. Der Administrator kann das gestohlene oder verlorene Gerät aus der Ferne lokalisieren und, wenn nötig, einen Befehl zum Löschen des Geräts oder zum selektiven Löschen von Unternehmensdaten senden.

6.1. Gerät löschen

Daten auf dem Gerät können aus der Ferne gelöscht werden, indem ein „Wipe“-Befehl gesendet wird. Dies kann aus der Geräteübersicht heraus durchgeführt werden:
Verwaltung > Geräte > Geräteeinstellungen > Aktion auswählen

- **„Gerät löschen“**, um alle Daten auf dem Gerät zu löschen
- **„Enterprise Wipe“**, um nur Unternehmensdaten (Container) zu löschen



6.2. Gestohlenes oder verlorenes Gerät lokalisieren

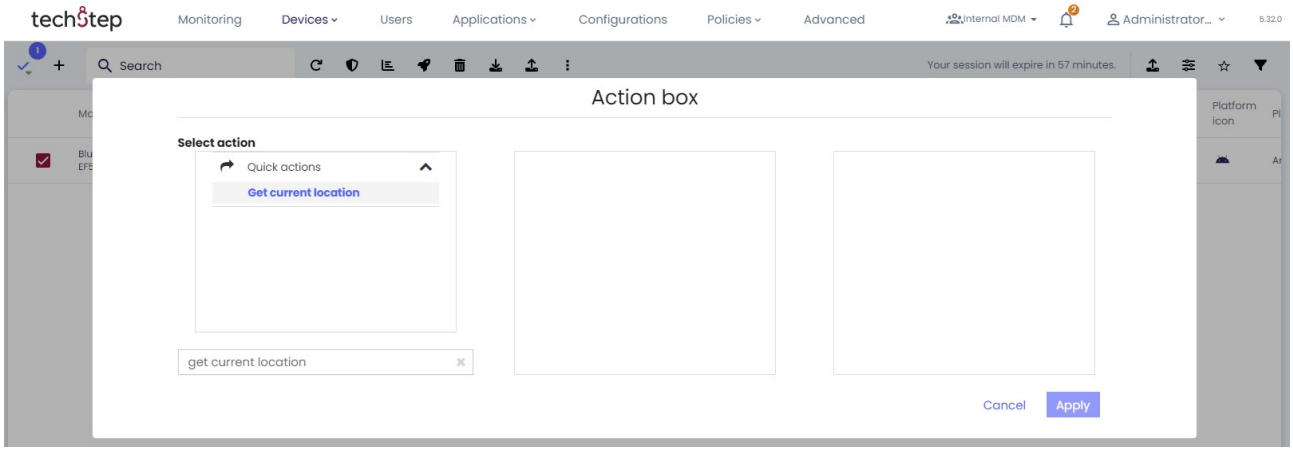
6.2.1. Android-Geräte

Das Gerät muss das Standortmodul installiert haben:

Richtlinien > Einstellungen ändern > Allgemeine Einstellungen > Standortdienste aktivieren

Falls das verwaltete Gerät gestohlen oder verloren geht und das Standortmodul installiert ist, kann der **datomo MDM**-Administrator das Gerät orten. Dies kann durch den Zugriff auf die Liste der Geräte erfolgen:

Verwaltung > Geräte > Geräteeinstellungen > Aktion senden > Aktuellen Standort abrufen.



6.2.2. Apple-Geräte

Um ein gestohlenes oder verlorenes Apple-Gerät zu lokalisieren, muss es in den „Verloren“-Modus versetzt werden - ab diesem Moment kann es lokalisiert werden.

Sie können ein Gerät in den „Verloren“-Modus setzen (nur im Supervised-Modus) über die Geräteübersicht:
Verwaltung > Geräte > Geräteeinstellungen > Aktion auswählen > Verloren-Modus aktivieren

Und dann:

Verwaltung > Geräte > Geräteeinstellungen > Aktion auswählen > Aktuellen Standort abrufen

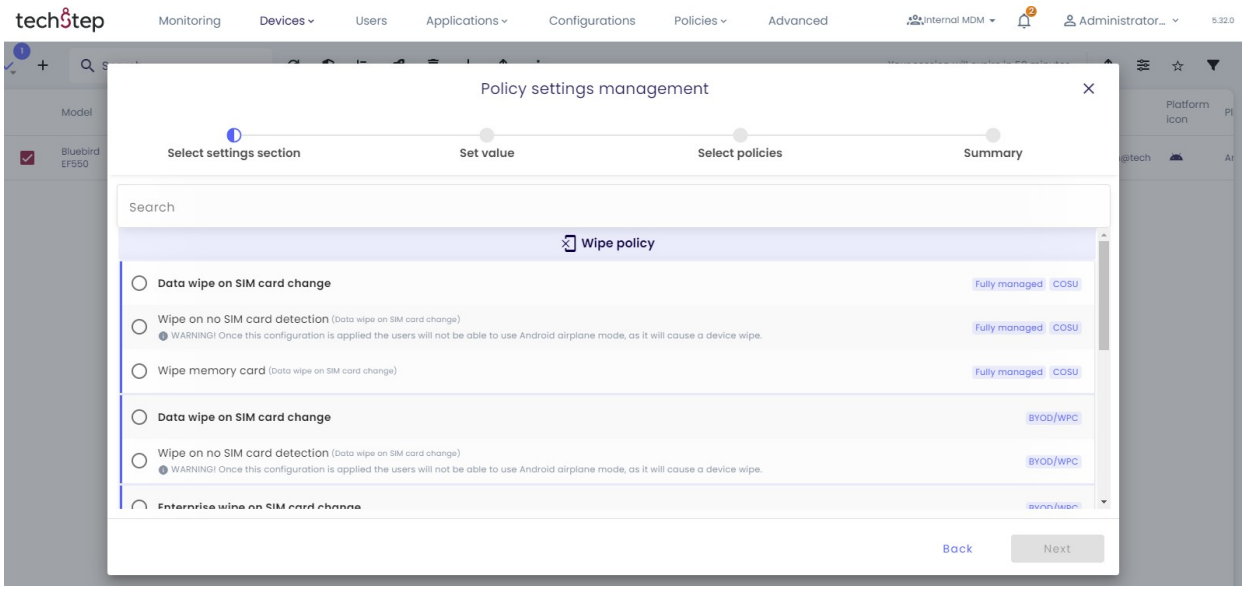
Wenn der „Verloren“-Modus aktiviert ist, wird das Gerät für den Endbenutzer gesperrt, bis es vom **datomo MDM**-Administrator entsperrt wird.

6.3. Automatische Datenlöschung

Der interne Speicher des Geräts kann im Falle eines Diebstahls oder Verlusts automatisch gelöscht werden, ohne dass der Administrator weitere Maßnahmen ergreifen muss. Die **datomo MDM**-Richtlinie kann so eingestellt werden, dass das Gerät im Fall der Entfernung oder Änderung der SIM-Karte automatisch gelöscht wird.

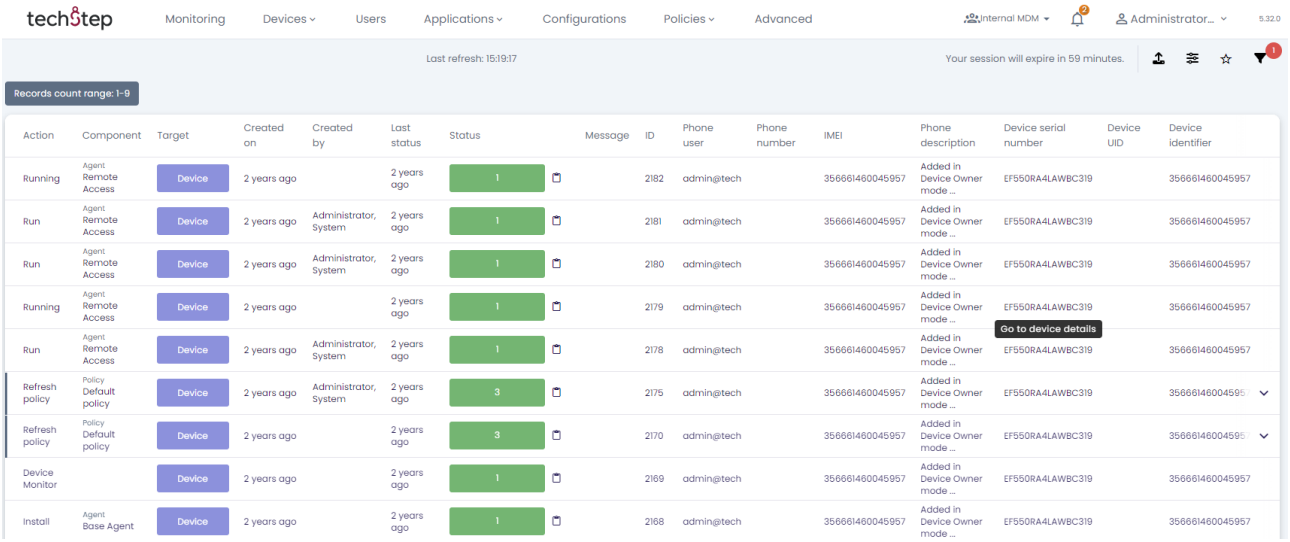
Zudem können Unternehmensdaten automatisch gelöscht werden, wenn die Sicherheit auf iOS (Jailbreak) oder Android (Root) gefährdet wird.

Richtlinien > Einstellungen ändern > Löschrichtlinie



6.4. Übersicht der Vorgänge in der Web-Konsole

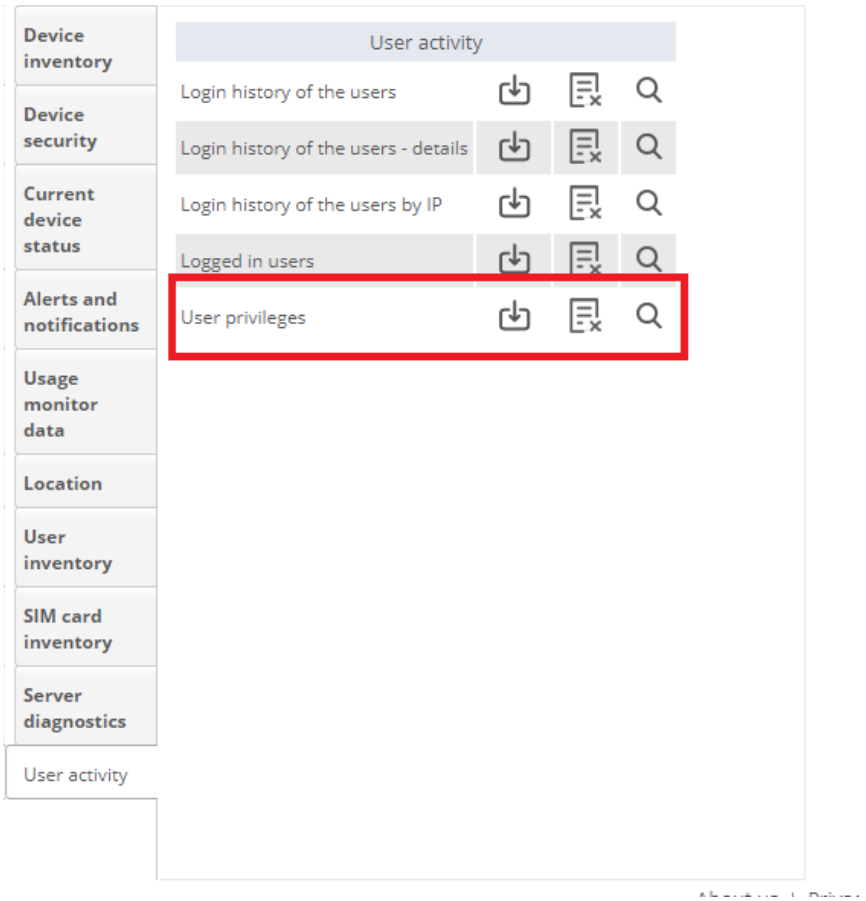
Alle von Administratoren im **datomo MDM**-System ausgeführten Vorgänge oder automatisch durch das System generierten Vorgänge basierend auf den Präferenzen werden gespeichert und sind im Log-Verlauf einsehbar. Der Log zeigt den Vorgangstyp, wer ihn durchgeführt hat, wann er ausgeführt wurde und seinen Status. Um die Liste der Vorgänge zu öffnen, gehen Sie zum Tab Log: **Geräte > Log**.



6.5. Übersicht der Benutzerberechtigungen

Jeder Benutzer, der sich im **datomo MDM**-System anmeldet, hat Berechtigungen, die ihm vom IT-Administrator des Unternehmens zugewiesen wurden. Diese Berechtigungen können potenziellen Zugriff auf private Daten gewähren. Sie können die Berechtigungen für einen bestimmten Benutzer im **datomo MDM**-System einfach einsehen.

Um einen Bericht für jeden Benutzer anzuzeigen, gehen Sie zu:
Erweiterte Optionen > Berichte > Benutzeraktivität > Benutzerberechtigungen


Device inventory
Device security
Current device status
Alerts and notifications
Usage monitor data
Location
User inventory
SIM card inventory
Server diagnostics
User activity
User activity
Login history of the users
Login history of the users - details
Login history of the users by IP
Logged in users
User privileges